Windows Media Player – HTML Hosting Threat Model

Program Manager: Kevin Larkin

Agenda

- What is HTML Hosting?
- Walk Through Threat Model for HTML Hosting
- Challenges with Threat Modeling

What is HTML Hosting?

What is HTML Hosting?

- **Areas Where Windows Media Player Hosts HTML**
  - Media Guide
  - Services
  - Captioning
  - License Acquisition
  - Find Album Information (metadata)
  - HTMLView

Threat Modeling HTML Hosting

- Threat Model Based on Latest Tool from the Security Team
  - Steps:
    - Get Background Information
    - Identify the Entry Points and Assets
    - Identify Threats and Potential Vulnerabilities
    - Mitigate

Background Information

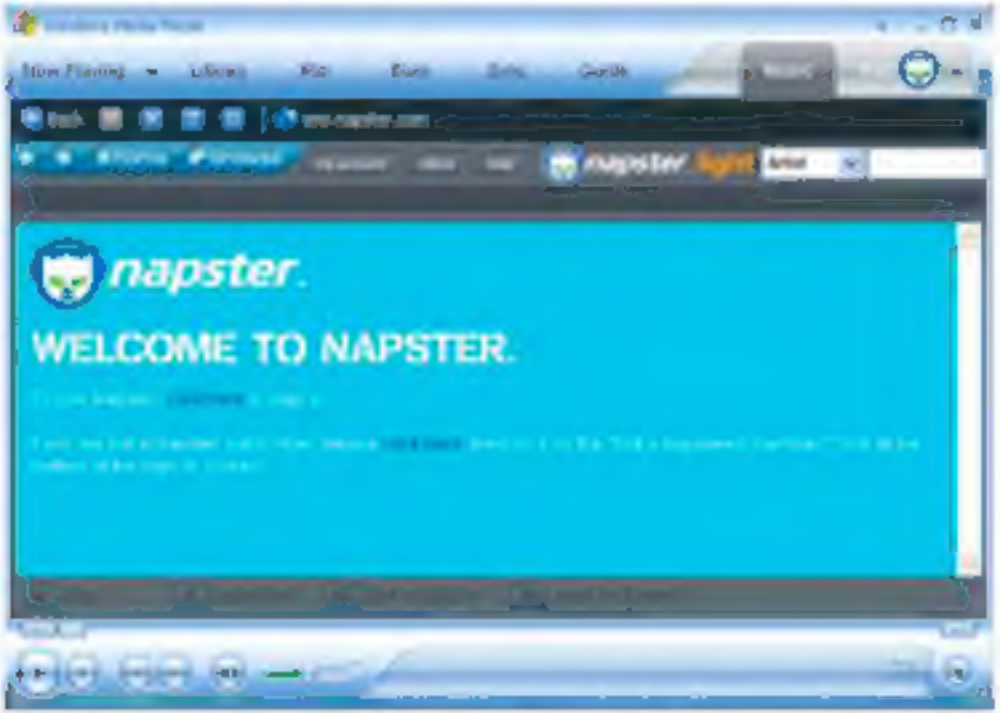
- Use Scenarios
- External Dependencies
- Implementation Assumptions
- External Security Notes
- Internal Security Notes

Use Scenarios

- Media Guide from WindowsMedia.com

Use Scenarios

- 3rd Party Services can set URLs to load HTML

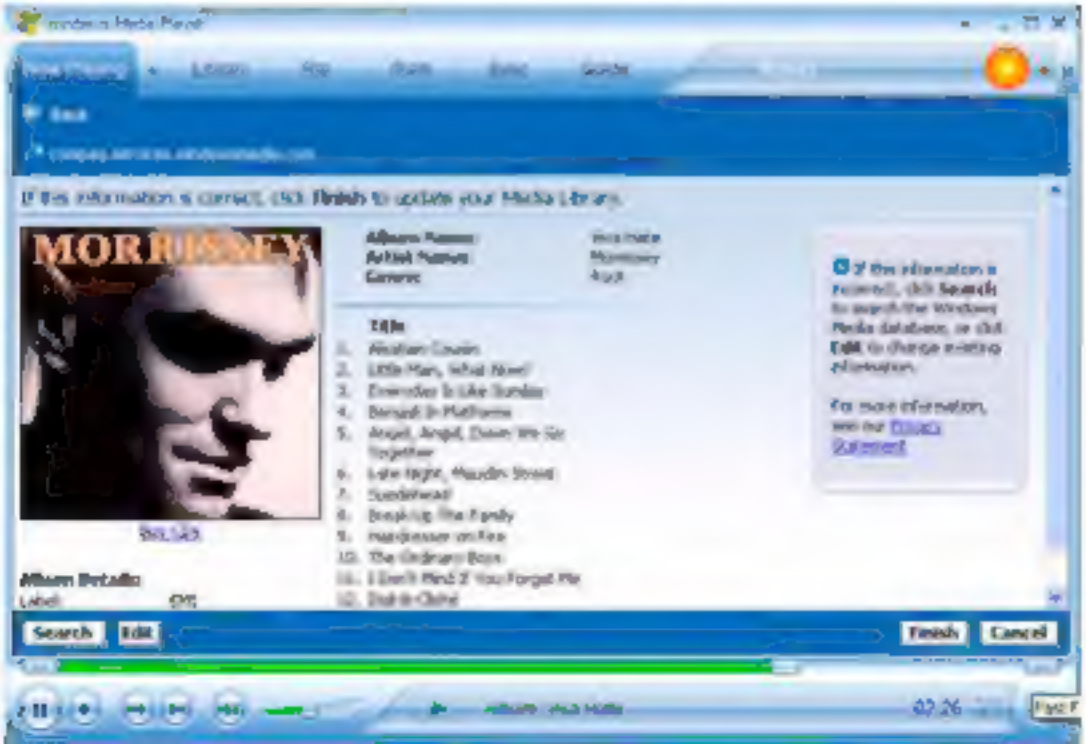


Use Scenarios

- ASX content plays (HTMLView)

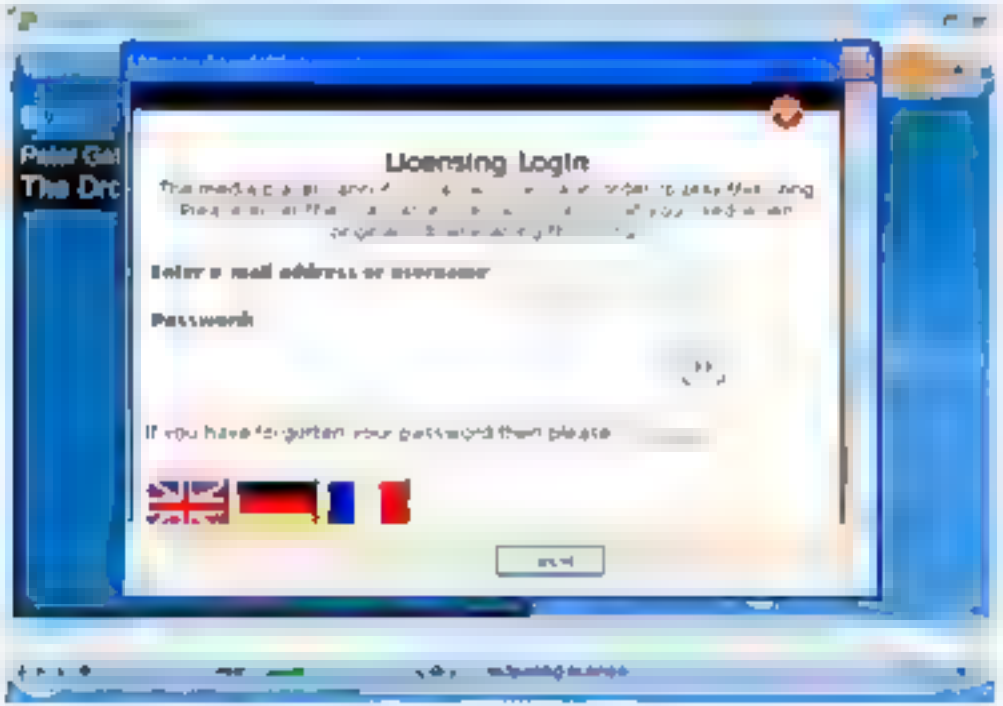
Use Scenarios

- HTML page is loaded from WindowsMedia.com (Get Names)



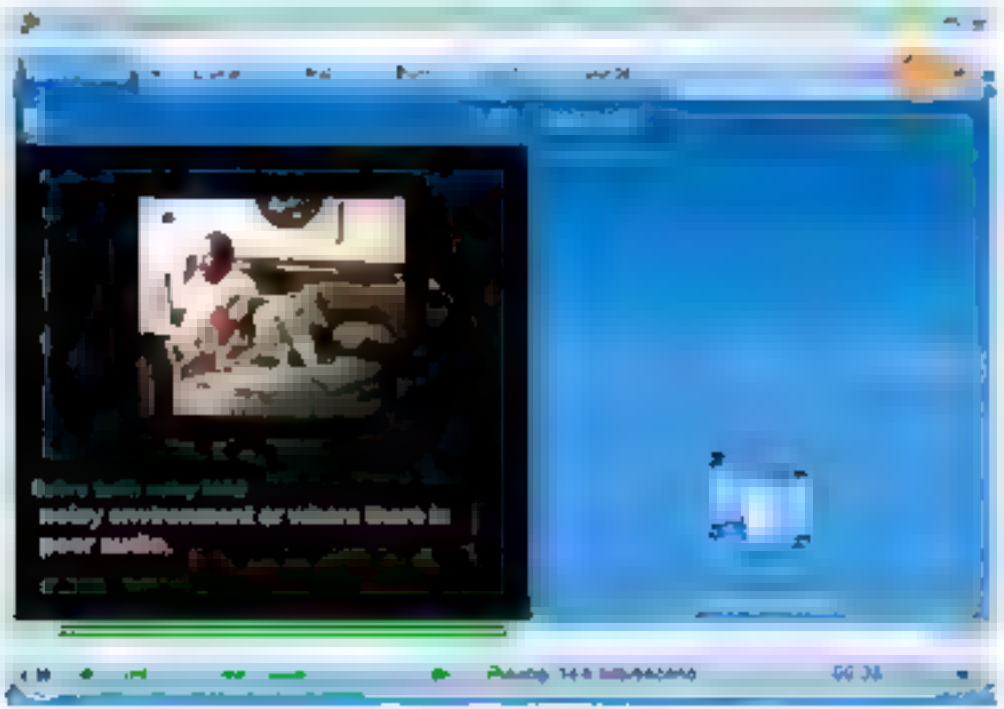
Use Scenarios

- License Acquisition



Use Scenarios

- Captioning



Use Scenarios

- HTML hosted in player should always be internet zone
- Player uses IE settings for setting security zone
- HTML hosted in the Player can embed the WMP ActiveX control and get a pointer to the remoted Player Core
- HTML hosted in the player can get access to the currently playing file only.

Scenarios

- A Win32 application using public APIs can remote the Player and set the HTML for task panes in the player user IWMPPlayerServices setTaskPaneURL
- HTML pages loaded in the player get access to an External Object depending on the Task Pane they are in
- Premium Services HTML get access to an External Object from the Player that provides a pointer to the Download Manager COM object and to NavigateTaskPane and SelectTaskPane APIs The CD/DVD task gets a similar but different External Object

Scenarios

- Script commands (URLs and FILENAME) from an Embedded OCX in Player hosted HTML should never fire in the Player
- Web Stream content from an Embedded OCX in Player hosted HTML should never render when in the Player
- Corporation sets group policies to turn off features that require web access and to lock the player to a skin

External Dependencies

- Internet Explorer DOM (Browser Object)
- Player OCX host detection mechanism and security wrapper
- WinInet API for determining security zone of web pages
- The Player uses IE's InternetSecurityManager to apply and manage security settings on HTML hosted in the Player
- WMIS(Media Guide etc) provides HTML as a service hosted in the player

Implementation Assumptions

- Microsoft Internet Explorer 6 Gold or better
- XP only: gold, sp1, sp2, home and professional (will not install on server)

External Security Notes

- Changing IE's privacy and security zone settings will directly impact how the Player hosts HTML pages. This includes cookies, trusted and restricted sites.
- The Player Privacy Statement outlines features and issues around player and services usage.

Internal Security Notes

Entry Points and Assets

- Trust Levels
- Entry Points
- Protected Resources
- Data Flow Diagrams

Trust Levels

- **Logged on User**
  - Most of WMP processes run in the context of the logged on user (Admin, restricted user, etc)
- **3rd Party Win32 App**
  - 3rd party apps may call the Player remoting APIs via the remote OCX and these apps are running with potentially any privilege level

Trust Levels

- Internet Web Page
  - HTML from an intranet or Internet web site will be loaded in Internet security zone
- Restricted Web Page
  - IE's restricted site settings are respected
- Trusted Web Page
  - IE's trusted site settings are respected

Entry Points

- **WindowsMedia.com**
  - Media Guide, Radio Tuner, Find Album Info
- **3rd Party Service**
  - Service Pane, Radio Tuner, Info Center
- **ASX / HTMLView**
  - URL to HTML file in ASX file
- **Service XML**
  - XML loaded by player to enumerate services

Entry Points

- 3rd Party Application
  - setTaskPaneURL
- Windows Media File
  - Captions come from script command stream in WMA, WMV, ASF files
- SAMI
  - Caption text read from associated SAMI file
- WMPLoc.dll
  - HTML loaded from WMP resources

Entry Points

- DRM HTML
  - Version 7 X license acquisition HTML
- OCX
  - Remoted OCX and WMPCore
- SetTaskPaneURL
  - SetTaskPaneURL public API
- NavigateURL
  - NavigateURL public API

Entry Points

- **WMP HTML Host**
  - The component in the player that hosts all HTML pages
- **IWMPExternal**
  - External object for services and CD/DVD pane

Protected Resources

- Media Library
  - The library of records that is the database for all the users music, video, and photo content and metadata.
- Media File
  - The physical music, video, and photo files and included metadata
- User Credentials
  - User credentials should not be exposed or modifiable

Protected Resources

- CPU
  - Want to avoid DoS attacks that consume CPU resources inappropriately Also avoid alien code running rogue process.
- RAM
  - Want to avoid attacks that corrupt RAM, or consume it inappropriately.
- Hard drive
  - Don't allow attacks to fill HD or corrupt data on the HD

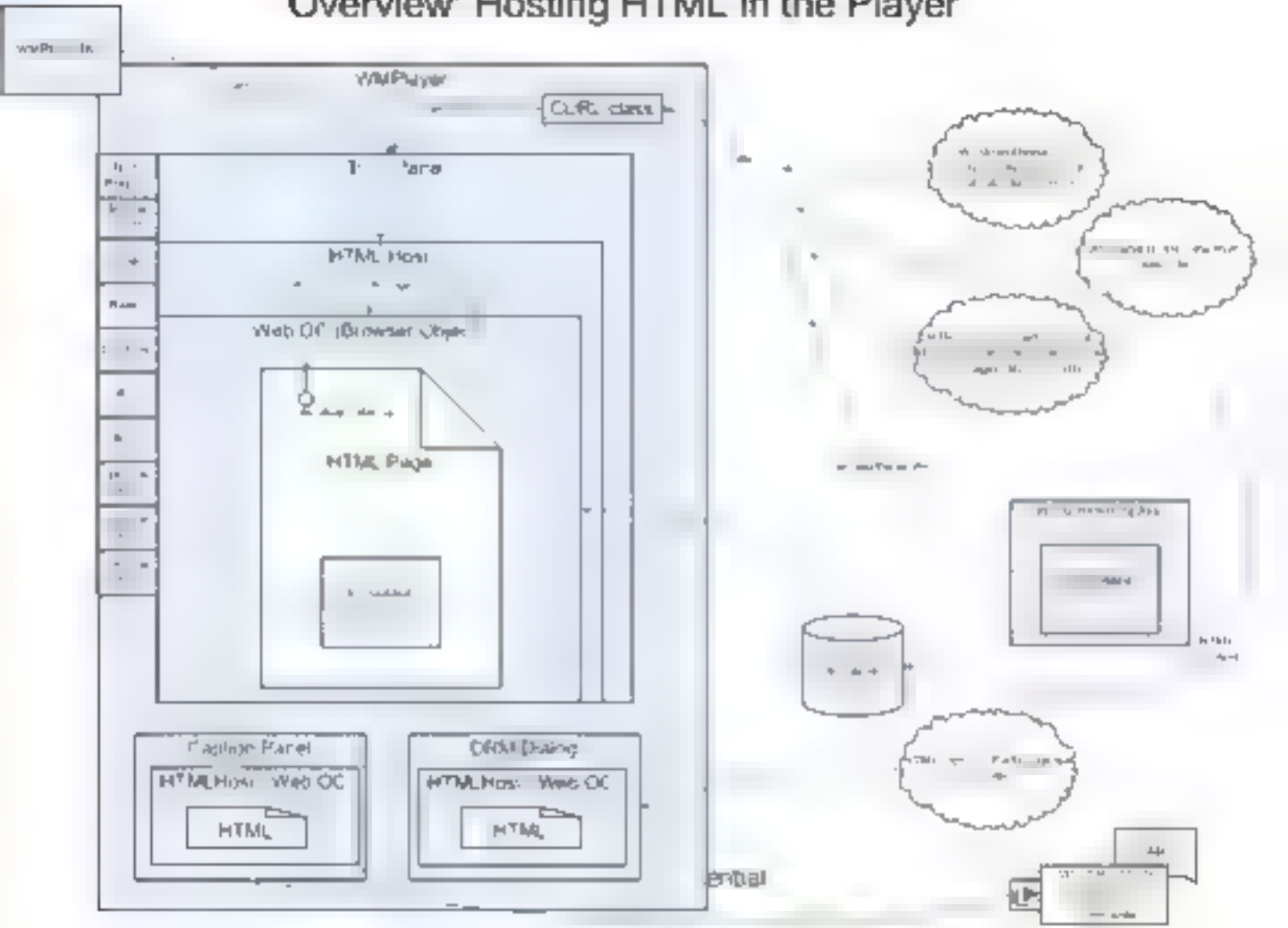
Protected Resources

- LAN and Intranet
  - Don't allow inappropriate discovery/access of LAN/Intranet Resources on the network.
- System/User Registry
  - System and User registry should be protected from inspection/corruption
- IE Cache
  - Contents of Internet Explorer's cache.

Protected Resources

- WMPLOC.dll
  - The DLL holds all the players resources and info about where to get services list, etc.
- WMP UI
  - WMP UI and User Experience

Overview: Hosting HTML in the Player



Threats

- Threats are Identified
- Potential Vulnerabilities are Identified and Investigated
- Bugs Entered for Non-Mitigated Vulnerabilities
- Bugs Triaged and Fixed

Threats Identified

- HTML/XML data coming into the Player from the network is spoofed
  - Player loads XML from WMIS to identify available services
  - Player loads HTML provided by service
- HTML hosted in the player gains local zone access or elevated privilege
- HTML hosted in the player is less secure than IE
- Cross Domain Scripting
- Navigation away from Service HTML
- Remoted OCX
- HTML Spoofing
- Local code messes with Player
- Data Leakage (one web page accessing another's data)
- Script commands fired in the Player from the OCX or from LaunchURL() are loaded in the Player

Potential Vulnerabilities Identified

- **Examples**:
  - Un-trusted or trusted site spoofs the Player or and gets user credentials, etc
  - User unaware of trust level of Web page being viewed
  - HTML exploits are not reputable, traceable
  - WMPLoc.dll gets tampered with
  - Issues with the handling of Cookies

Some Key Mitigations

- Bugs entered for each vulnerability to investigate
- Some Key Mitigations
  - Ensuring our HTML Hosting is as Secure as new IE Security Features
  - Locking down player to not allow Local Zone HTML access
  - Warning the user before displaying un-expected HTML
  - Displaying an icon on with HTML pages that show whether the connection is secure
  - Allowing users to see the base URL for HTML pages

Challenges with Threat Modeling

- Previously Released Features
- End User – Ease of Use
- Dependencies
- The Bar Keeps Raising

Questions?